Lab 10.1: Cifrado de discos

En este ejercicio usted cifrará una partición en el disco para proveer de seguridad en caso de que su disco duro o portátil es robado. Revisar la documentación de **cryptsetup** antes de comenzar es una buena idea (`man cryptsetup` y `cryptsetup --help`).

1. Cree una partición nueva para el dispositivo de bloque cifrado con **fdisk**. Asegúrese que el kernel está al tanto de la nueva tabla de partición. Un reinicio lo logrará, pero hay otros métodos también.
2. Formatee la partición con **cryptsetup** usando **LUKS** para la capa de cifrado.
3. Cree la clave para abrir el dispositivo de bloque cifrado.
4. Agregue una entrada a /etc/crypttab para que el sistema pregunte la clave en el reinicio.
5. Formatee el sistema de archivos con **ext4**.
6. Cree un punto de montaje para el sistema de archivos nuevo, por ejemplo /secret.
7. Agregue una entrada a /etc/fstab para que el sistema sea montado en el arranque.
8. Intente montar el sistema cifrado.
9. Reinicie y valide la configuración completa.

Solution 10.1

1. `$ sudo fdisk /dev/sda`

   Cree una partición nueva (en el ejemplo trabajaremos con /dev/sda4) y luego ejecute:

   `$ sudo partprobe -s`

   para que el sistema relea la tabla de partición modificada, o reinicie (lo cual es lejos lo más seguro).

   Nota: Si no puede usar una partición real, use el método descrito en el capítulo anterior para trabajar con un dispositivo loop o un archivo de imagen.

2. `$ sudo cryptsetup luksFormat /dev/sda4`

3. `$ sudo cryptsetup luksOpen /dev/sda4 secret-disk`

4. Agregue lo siguiente a /etc/crypttab:

   ```
   secret-disk    /dev/sda4
   ```

5. `$ sudo mkfs -t ext4 /dev/mapper/secret-disk`

6. `$ sudo mkdir -p /secret`

7. Agregue lo siguiente a /etc/fstab:

   ```
   /dev/mapper/secret-disk    /secret    ext4    defaults    1 2
   ```

8. Monte el sistema de archivos:

   `$ sudo mount /secret`

   o monte todos los sistemas de archivos mencionados en /etc/fstab:

   `$ sudo mount -a`

9. Reinicie.

